REMARKS

In accordance with the foregoing, claims 1, 2, 7, 8, 10, and 12-15 are amended to improve clarity and new claims 16-26 have been added.

Claims 1-26 are pending and under consideration.

CLAIM OBJECTIONS:

In the Office Action, at page 2, claims 7 and 15 were objected to for informalities. The claims have been amended to improve clarity. Accordingly, it is respectfully requested that the objections to the claims be withdrawn.

REJECTION UNDER 35 U.S.C. § 102:

In the Office Action, at page 3, claims 1-12 were rejected under 35 U.S.C. § 102 in view of U.S. Patent No. 6,185,316 to Buffam ("Buffam"). The reasons for the rejection are set forth in the Office Action and therefore not repeated. The rejection is traversed and reconsideration is requested.

Buffam generally describes a comparator including a decoder that removes a claimant true image points from the information points and produces proffered false image points. See column 8, lines 28-38. The decoder extracts a decoding key from the proffered false image points using the key to decode the ciphertext therewith and produced proffered plaintext. However, the cited reference fails to teach or suggest that the decoding key is generated "for decrypting said cryptographic key, from said **encrypted physical characteristic information and** said **numeric key**," emphasis added, as recited in independent claim 1. Nothing in Buffam teaches or suggests the generation of the auxiliary code. One of the many advantages of generating the auxiliary code as recited in independent claim 1 is that the numeric key based on the cryptogram itself may be restored, and such cryptogram may be generated to prevent a restoration of the numeric key by partially altering itself in the transmittance process.

Independent claim 3 recites, "code generating means for generating an auxiliary code from said encrypted physical characteristic information and said numeric key," and claim 5 recites, "a code generating procedure for generating an auxiliary code from said encrypted physical characteristic information and said numeric key." Because independent claims 3 and 5 include similar claim features as those recited in independent claim 1, although of different scope, the arguments presented above supporting the patentability of independent

claim 1 are incorporated herein to support the patentability of independent claims 3 and 5.

Referring to independent claim 2, the decoder of Buffam extracts a decoding key from the proffered false image points using the key to decode the ciphertext therewith and produced proffered plaintext. However, the cited reference fails to teach or suggest "restoring a numeric key from said received encrypted physical characteristic information **and** said auxiliary code," emphasis added, as recited in independent claim 2. Nothing in Buffam teaches or suggests the restoration of the numeric key. Rather, the decoding key is only means used to decode.

Independent claim 4 recites, "numeric key restoring means for restoring a numeric key from said encrypted physical characteristic information and said auxiliary code," and claim 6 recites, "a numeric key restoring procedure for restoring a numeric key from said encrypted physical characteristic information and said auxiliary code." Because independent claims 4 and 6 include similar claim features as those recited in independent claim 2, although of different scope, the arguments presented above supporting the patentability of independent claim 2 are incorporated herein to support the patentability of independent claims 4 and 6.

Referring to independent claim 7, Buffam generally provides a key generator for creating a substantially random encoding key from the false information points using a preselected key generation technique, for example, hashing. See column 8, lines 1-11. The cited reference also obtains a master template from the original image and provides an encoder to produce ciphertext from plaintext input to the encoder, responsive to the encoding key. In addition, the apparatus of Buffam may be tailored to suit a desired level of security through self-authentication. See column 14, lines 30-44. However, the cited reference fails to teach or suggest all the claimed features recited in independent claim 14. For instance, the cited reference fails to teach or suggest, "**arithmetically converting** each component of said physical characteristic information by using a predetermined function concerning said each component and a plurality of components having a predetermined relationship with said each component, **to scramble** said physical characteristic information," emphasis added, as recited in independent claim 7. Rather, Buffam limits its description to providing a size of true image points (TIP) set representing an original image, a length of the encryption key represented by the encoded image points, and a number of missing data points in the decoded TIPs set selectable and subject to policy decisions. See column 14, lines 30-44. Buffam is silent as to providing the arithmetic conversion and the scramble of "said physical characteristic information," as recited in independent claim 7.

Independent claim 9 recites, "scrambling means for arithmetically converting each

component of said physical characteristic information by using a predetermined function concerning said each component and a plurality of components having a predetermined relationship with said each component, to scramble said physical characteristic information," and claim 11 recites, "a scrambling procedure for arithmetically converting each component of said physical characteristic information by using a predetermined function concerning said each component and a plurality of components having a predetermined relationship with said each component, to scramble said physical characteristic information." Because independent claims 9 and 11 include similar claim features as those recited in independent claim 7, although of different scope, the arguments presented above supporting the patentability of independent claim 7 are incorporated herein to support the patentability of independent claims 9 and 11.

The present invention recognizes that a final result of decoding obtained from an unauthorized cryptogram, which is made by partially altering the cryptogram is fluctuated to such an extent that it becomes very different from the original physical characteristic information, by descrambling a result of decoding through a conversion using an inverse function of the appropriate function. However, Buffam fails to recognize the problems that the present invention targets. And, accordingly, the cited reference fails to teach or suggest, "descrambling said scrambled physical characteristic information by removing each element from each component constructing the result of decryption, in which each element is effected at the time of scrambling, by a plurality of components that has a predetermined relationship with said each component," as recited in independent claim 8.

By merely providing a decoder removing true image points from information points and extracting a decoding key from false image points using the key, and comparing an original plaintext with a proffered plaintext with an authenticating signal, Buffam fails to teach or suggest, "descrambling said scrambled physical characteristic information by removing each element from each component constructing the result of decryption, in which each element is effected at the time of scrambling, by a plurality of components that has a predetermined relationship with said each component," as recited in independent claim 8.

Independent claim 10 recites, "decrypting means for decrypting a received cryptogram which is an encryption of a scrambled physical characteristic information, by a predetermined cryptographic key and obtaining said scrambled physical characteristic information; and descrambling means for descrambling said scrambled physical characteristic information," and claim 12 recites, "a decrypting procedure for decrypting a received cryptogram which is an encryption of a scrambled physical characteristic information, by a predetermined

cryptographic key and obtaining said scrambled physical characteristic information; and a descrambling procedure for descrambling said scrambled physical characteristic information." Because independent claims 10 and 12 include similar claim features as those recited in independent claim 8, although of different scope, the arguments presented above supporting the patentability of independent claim 8 are incorporated herein to support the patentability of independent claims 10 and 12.

Because new independent claims 16-23 include similar claim features as those recited in independent claims 1-12, although of different scope, the arguments presented above supporting the patentability of independent claims 1-12 are incorporated herein to support the patentability of new independent claims 16-23.

In view of the foregoing, it is respectfully asserted that independent claims 1-23 are patentable in view of Buffam. Accordingly, it is respectfully requested that independent claims 1-23 be allowed.

REJECTION UNDER 35 U.S.C. § 103:

In the Office Action, at page 6, claims 13-15 were rejected under 35 U.S.C. § 103 in view of Buffam and further in view of U.S. Patent No. 5,799,088 to Raike ("Raike"). The reasons for the rejection are set forth in the Office Action and therefore not repeated. The rejection is traversed and reconsideration is requested.

Buffam generally provides a fingerprint-based authentication using as an input structure or image sensor any sensor that can provide an image or structural representation that is unique to the user. See column 11, line 58, to column 12, line 3. In addition, the cited reference provides a key generator for creating a substantially random encoding key from the false information points using a preselected key generation technique, for example, hashing. See column 8, lines 1-11. Referring to Raike, this reference generally describes that although a public-key system is inherently less dependent upon such factors for its security than conventional or private-key systems. If a private key is stored anywhere in a computer or data storage system, physical security becomes an important issue.

However, Buffam and Raike, individually or combined, fail to teach or suggest, "proof information inputting means for inputting information including identifier or identifying the individual and a password, encrypting means for encrypting said physical characteristic information using said password as a cryptographic key and outputting a cryptogram," as recited

in independent claim 13. The Office Action relied on Raike as providing the use of a password, however, this reference fails to teach or suggest that such password is used "for encrypting said physical characteristic information" and that said password is used "as a cryptographic key," as recited in independent claim 13.

Buffam generally provides authenticating indicia and verifying the image thereby. One particular embodiment is a biometric application such as a fingerprint-based authentication system. See abstract. The apparatus includes an image receiver for receiving the original image with true image point, a false image point generator providing false image points, and a transient template generator that selectively combines the true image points and the false image points. In contrast, Raike generally describes a non-deterministic public key encryption system whereby a public key is generated from a private key using mathematical operations equivalent to exponentiation in finite fields. Thus, an attacker is required to compute logarithms over finite fields. The Office Action correctly recognized that Buffam fails to teach or suggest, "decrypting means for decrypting said received cryptogram by using the password retrieved by said retrieving means as a cryptographic key and obtaining a physical characteristic information," as recited in independent claim 13. Accordingly, the Office Action conclusively asserted that the description of Raike should be included into Buffam to arrive to the claimed features of the presently claimed invention.

However, there is no motivation in Buffam to incorporate therein the descriptions provided in Raike. Further, the Office Action merely indicates, "it would have been obvious to one of ordinary skill in the art at the time the invention was made to use the teaching of Raike by using a password to generate a cryptographic key to speed up the key generation process." However, it is improper to merely indicate that a feature is obvious. There **must** be supporting rationale and discussion laying out the case using the cited references for such a conclusion.

Nothing in either reference suggests or supports the purported combination of the references set forth in the Office Action. It is submitted that the reason why no such showing was made is because the prior art of record individually or combined, fail to teach, suggest, or otherwise provide the motivation needed to make such a modification. "To support the conclusion that the claimed combination is directed to obvious subject matter, either the references must expressly or impliedly suggest the claimed combination. It is to be noted that simplicity and hindsight are not proper criteria for resolving the issue of obviousness." Ex Parte Clapp, 227 USPQ 972, 973 (B.P.A.I. 1985).

Accordingly, in view of the foregoing, it is respectfully asserted that the prima facie

obviousness rejection fails on its face and, accordingly, Buffam and Raike fail to teach or suggest a trading card comprising "proof information inputting means for inputting information including identifier or identifying the individual and a password, encrypting means for encrypting said physical characteristic information using said password as a cryptographic key and outputting a cryptogram," as recited in independent claim 13.

Thus, even assuming, arguendo, that Buffam and Raike were combined, the combination would be silent as to providing the claimed features of the recording and/or reproducing unit recited in independent claim 13.

Independent claim 14 recites, "proof information inputting means for inputting information including identifier or identifying an individual and a password; encrypting means for encrypting said physical characteristic information using said password as a cryptographic key and outputting a cryptogram," and claim 15 recites, "decrypting means for decrypting said received cryptogram by using the password retrieved by said retrieving means as a cryptographic key and obtaining a physical characteristic information." Because independent claims 14 and 15 include similar claim features as those recited in independent claim 13, although of different scope, the arguments presented above supporting the patentability of independent claim 13 are incorporated herein to support the patentability of independent claims 14 and 15.

Because new independent claims include similar claim features as those recited in independent claims 13-15, although of different scope, the arguments presented above supporting the patentability of independent claims 13-15 are incorporated herein to support the patentability of new independent claims 24-26.

In view of the foregoing, it is respectfully asserted that independent claims 13-26 are patentable in view of Buffam and Raike. Accordingly, it is respectfully requested that independent claims 13-26 be allowed.

CONCLUSION:

In accordance with the foregoing, it is respectfully submitted that all outstanding objections and rejections have been overcome and/or rendered moot, and further, that all pending claims patentably distinguish over the prior art. Thus, there being no further outstanding objections or rejections, the application is submitted as being in condition for allowance, which action is earnestly solicited.

If the Examiner has any remaining issues to be addressed, it is believed that prosecution can be expedited by the Examiner contacting the undersigned attorney for a telephone interview to discuss resolution of such issues.

If there are any underpayments or overpayments of fees associated with the filing of this Amendment, please charge and/or credit the same to our Deposit Account No. 19-3935.

Respectfully submitted,

STAAS & HALSEY LLP

Date: February 24, 2004

By: 

Alicia M. Choi
Registration No. 46,621

1201 New York Avenue, NW, Suite 700
Washington, D.C. 20005
Telephone: (202) 434-1500
Facsimile: (202) 434-1501